Countermeasures to Prevent Eavesdropping on Unintentional Emanations from Personal Computers

Yasunao Suzuki[†], *Masao Masugi, Kimihiro Tajima, and Hiroshi Yamane*

Abstract

This article outlines the scheme that we have developed as a countermeasure to prevent information leakage through eavesdropping on emanations emitted by personal computers (PCs). It also describes the present performance of our current prototype. A working PC usually produces unintentional electromagnetic fields, and some of these emissions often carry significant information about what is being processed in the PC. In some cases, the content being shown on the screen of a video display unit could be reconstructed by intercepting such emissions at a distance.

1. Background

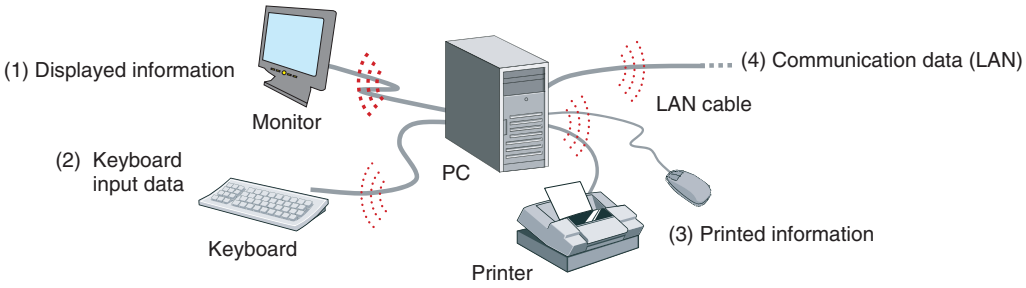
Electronic equipment, such as communication equipment or personal computers (PCs), usually emits unintentional radiated electromagnetic fields when it is working and these affect other equipment nearby. Conversely, the performance of such equipment is often degraded by emissions present around it. These phenomena also enable malicious persons to conduct many kinds of attacks on information security, such as eavesdropping on information leaked by these emanations or harming hardware by irradiating it with powerful fields in order to cause malfunctions or physical damage. These problems caused by electromagnetic waves are referred to as *electromagnetic security problems*.

With the recent rapid progress of electronic technologies, the speed of signals being processed in electronic circuits has increased, and the maximum frequency of the emanations from these circuits has correspondingly increased. These emitted electromagnetic waves often carry significant information about the data being processed inside the equipment. In some cases, this hidden information can be reconstructed by intercepting such emissions, as a result of improvements in radio receiver performance and advances in signal processing techniques. Consequently, this topic represents a potential new information security threat [1], [2].

† NTT Energy and Environment Systems Laboratories
Musashino-shi, 180-8585 Japan

2. TEMPEST—Eavesdropping on PC display information

Information on a PC screen can be remotely reconstructed exactly as it appeared on the display by monitoring and appropriately demodulating the weak emanations generated by the PC and its peripheral equipment [1]. Such an eavesdropping technique had been researched by some military organizations since around 1960, but most of the results were classified and not disclosed to the public. It came to public attention in 1985 when Wim van Eck pointed out that information on a cathode ray tube display can easily be reconstructed [2]. Since his work, research on information leakage of this kind has been conducted by many organizations. The National Security Agen-



Information hidden in leaking emissions	Importance and quantity of the information	Difficulty of regenerating original information	Strength of emissions	Total threat of information leakage
(1) Displayed information	High (displayed information)	Easy	Strong	High
(2) Keyboard input data	Low to medium (only text)	Hard (need to decipher code assigned to each key)	Weak	Low to medium
(3) Printed information	Low (only printed information)	Hard (need to demodulate printer interface signal)	Weak	Low
(4) Communication data	Medium to high (communicated information)	Hard (need to demodulate LAN interface signal)	Weak	Medium

LAN: local area network

Fig. 1. Types of information hidden in leaking emissions and the treatment of information leakage.

cy (NSA) in the USA refers to this type of threat by the covername TEMPEST, and this term is now in general use [3].

2.1 Threat and features of TEMPEST

Several kinds of security problems are caused by electromagnetic radiation (**Fig. 1**). For example, it has reported that the key hit by an operator on a keyboard could be deciphered, and, as another example, a printed image could reconstructed by receiving emanations leaking from a laser printer. However, the field strengths of these emanations are weaker than those of the display signals, so it is difficult to decode the original signals from these emanations.

On the other hand, eavesdropping on emitted video signals seems to pose a greater risk than the other electromagnetic security problems. This is because the information that appears on PC displays or other displays like automatic teller machine panels needs a high level of security in general, and there is much more of this information than of other types of information like text data and sound. Moreover, eavesdropping on leaking video signals can be done using simple and inexpensive equipment sold on the market if eavesdroppers have accurate knowledge about the eavesdropping technique.

Electromagnetic eavesdropping on unintentional emanations has some unique features. First, the information leakage is not discovered unless an eavesdropper is caught red-handed because it leaves no trace at all. Second, information can be stolen from PCs even when they are not performing data communications, such as using a wireless local area network.

2.2 TEMPEST countermeasure schemes

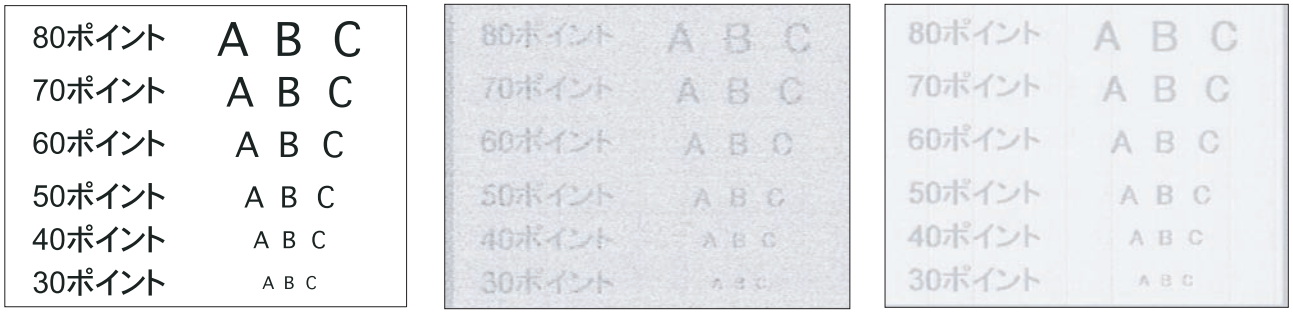
There are some conventional countermeasure schemes that can protect information from TEMPEST eavesdropping.

(1) Shielding

Shielding devices and/or rooms with metallic materials is a reliable way to reduce the leakage of emissions. However, it is difficult and expensive to achieve complete shielding, especially for the shielding of rooms and buildings.

(2) Soft tempest (using special fonts)

Soft tempest is a software-based countermeasure. It has been reported that the strength of emissions can be reduced by using specifically designed fonts, which make reconstructed text images hard to read



(a) Original display image on PC monitor

(b) Image reconstructed from emanations (not averaged)

(c) Image reconstructed from emanations (average of 32 frames)

Fig. 2. Reconstructed images.

[4]. This scheme is cost effective, but the fonts are sometimes insufficiently indistinct, and it has no effect on figures or drawings.

(3) Filtering

Inserting filters into communication interface cables or power supply cables to suppress emissions is also effective. However, these filters need to be inserted into all of the external interfaces and tuned to the emission frequency. Moreover, this method is effective only if the emissions are radiating mainly from the interface lines rather than from the PC itself.

(4) Jamming

Overlaying jamming electromagnetic fields that are stronger than leaking emanations is another effective countermeasure. This enables countermeasures to be taken using simple low-cost equipment and it is applicable for mobile use. However, the jamming signals should be chosen very carefully because the effectiveness of blocking eavesdropping depends strongly on the modulation pattern of the jamming signal.

We have developed a countermeasure device that uses the jamming technique to prevent the leakage of display information through unintentional emanations from PC displays. Below, we introduce the principle and functions of this device and describe how we verified its performance and applicability through experiments.

2.3 Video display interfaces for PCs

At present, the most popular video signal interfaces used for PC displays are ones standardized by VESA (Video Electronics Standards Association). The main analog-video interfaces—SVGA, XGA, and SXGA—are conventional analog raster scan video interfaces, and the video screen is constructed with pixels (minimum unit of drawing) drawn on the screen as the scanning line advances. Those video interfaces consist of three video signals corresponding to the colors red, green, and blue (RGB) and two synchronization signals: horizontal synchronization (H-sync) and vertical synchronization (V-sync). The basic time period for drawing a pixel on the video monitor is called the dot clock or pixel clock. The video signals are generated by modulating the amplitude of the dot clock pulse by the luminosity of the pixel. For example, the bit-rate of the dot clock is 65 Mbit/s for one case of XGA: when the number of pixels is 1024 × 768, H-sync frequency is 48.4 kHz, and V-sync frequency is 60 Hz.

2.4 TEMPEST eavesdropping on PC video display

The frequency spectrum of the emanations from a PC is widely spread and their intensity is very weak. Moreover, there are some meaningless signal components and/or noise in the emanations. Therefore, some special know-how and experience is required to reconstruct a PC display image by TEMPEST eavesdropping.

An example of display images intercepted by eavesdropping is shown in **Fig. 2**. The original display image on the PC monitor is shown in Fig. 2(a), and the image reproduced from detected emanations is shown in Fig. 2(b). These measurements and all of the following experiments were performed in an anechoic chamber at the distance of 3 m from the PC under test. The video-frame averaging technique is an effective way to reconstruct a clear image by diminishing the influence of random noise. Figure 2(c) is an image obtained by applying an averaging technique to the image in Fig. 2(b). In this case, the noise

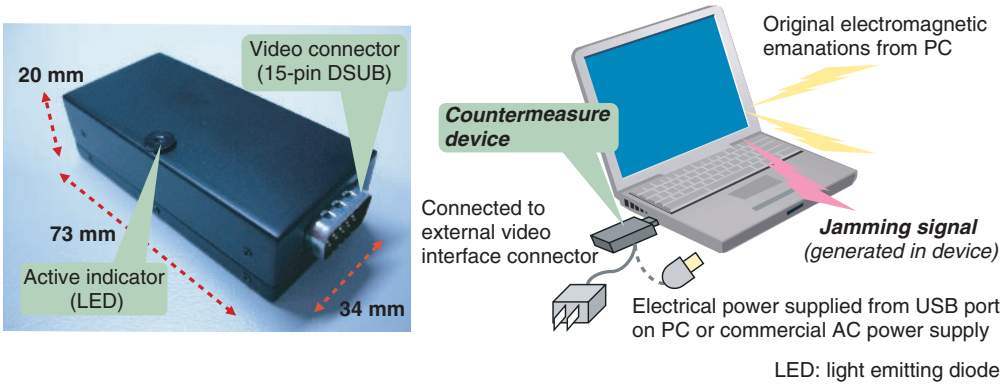


Fig. 3. TEMPEST Guard.

in a single video frame was diminished by averaging thirty-two video frames.

3. TEMPEST Guard—our information leakage countermeasure device

We have developed a device to prevent information leakage from PCs. The external appearance of a prototype is shown in **Fig. 3**. We call this device TEMPEST Guard because it guards against TEMPEST eavesdropping. It is connected to the external video interface connector of a PC and is powered either from one of the PC's USB (universal serial bus) ports or from the commercial AC power supply. If it intended for use with a desktop PC, an output video port is installed at the other end of the device and the monitor display is supplied by the video signal from this port.

3.1 Principle

TEMPEST Guard picks up the video signal from the external video display connector of a PC to regenerate the dot clock. This regenerated dot clock pulse is modulated to generate a jamming signal. The dot clock frequency varies from one PC to the next and also fluctuates according to the circumstances like the thermal condition of the PC. However, we can produce an effective jamming signal for a given PC under any circumstances by synchronizing its basic frequency with the original dot clock.

Thus, the obtained jamming signal is output into the external video display interface of the PC by common mode. This jamming signal interferes with the common-mode component of the video signal, which could be the origin of leakage emissions, and this makes it hard to reconstruct the original signal by eavesdropping. However, the normal-mode component, which actually draws the scanning line on the display, is not influenced by the jamming signal, so the original display remains in its original state. Both the jamming signal and the original video signal are emitted from the PC by the same radiation mechanism, so the radiation pattern of both emissions is almost the same.

To counteract the video-frame averaging technique, we modulate the jamming signal by a fixed pattern synchronized to both the horizontal and vertical synchronization signals. Such a jamming signal draws a fixed pattern on the monitor if it is reconstructed, and this fixed pattern is not diminished by the video-frame averaging scheme. Therefore, the jamming is effective even when video-frame averaging is applied.

3.2 Performance evaluation

An example of the frequency spectrum of the signal radiated by TEMPEST Guard (blue line) and the original emanation from a PC (red line) is shown in **Fig. 4**. The electric field strength of the TEMPEST Guard signal is much higher than the original signal, especially at the peak frequency that includes video signal information. This means that the jamming protection is effective over a wide frequency region.

Experimental results that confirm the effectiveness of jamming signal modulation are shown in **Fig. 5**. It shows reconstructed images of the original image (Fig. 2(a)) when the device's jamming signal was not modulated (Fig. 5(a)) and was modulated by a fixed pattern representing a vertical stripe image on the display (Fig. 5(b)). As can be seen in Fig. 5(b), information about the original image completely disappeared amid the high-contrast vertical stripes, even

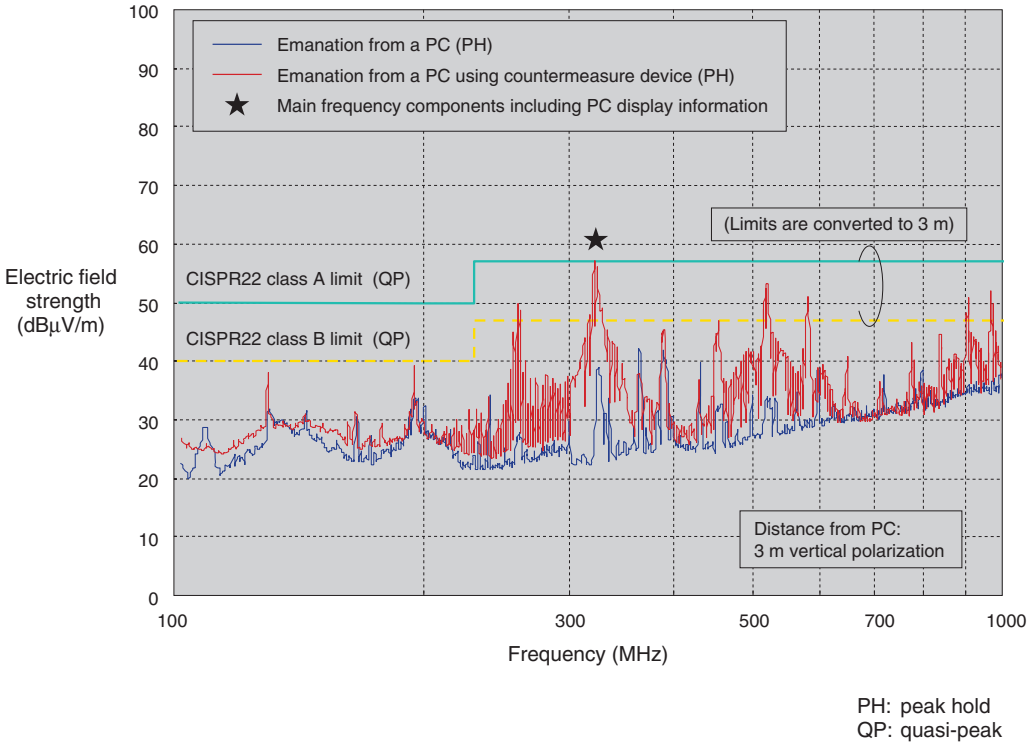
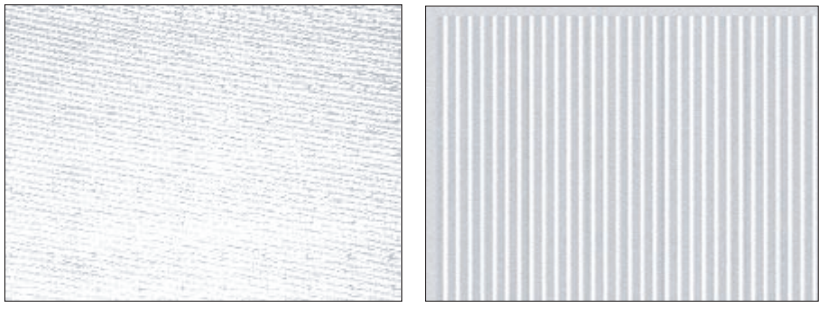


Fig. 4. Frequency spectrum of countermeasure device.



(a) For unmodulated jamming (b) For modulated jamming

*Original display image is the same as Fig. 2(a)).

Fig. 5. Performance of the countermeasure device revealed by images reconstructed from emanations.

when 32 video frames were averaged.

An example of a radiation pattern of TEMPEST Guard is shown in **Fig. 6**. It shows that the directional dependence of the electromagnetic field strength had a peak at 390 MHz. The field strength of TEMPEST Guard's jamming signal was almost isotropic and much higher than that of the emissions from a single PC in any direction from the PC's position. This means that the device effectively interfered with eavesdropping from any direction.

4. Conclusion

We have developed a portable countermeasure device called TEMPEST Guard to prevent eavesdropping on PC display information from intercepted unintentional emanations. It uses a jamming scheme and is effective for emissions of any frequency and in

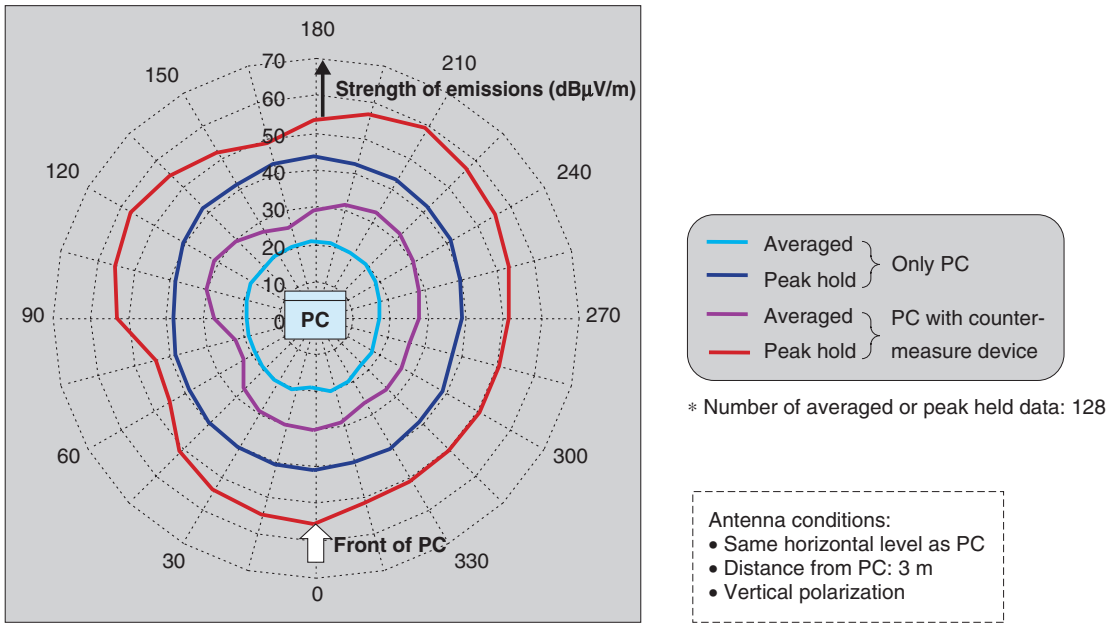


Fig. 6. Directional dependence of electromagnetic field strength.

any direction even when the video-frame averaging technique is used by the eavesdroppers. A study on a method of evaluating the jamming effect and a quantitative index for evaluating it are now in progress.

References

[1] Y. Suzuki, M. Masugi, K. Tajima, and H. Yamane, "Countermeasure Technique for Information Leakage by the Electromagnetic Emissions from Personal Computers," The 2008 Annual meeting IEE Japan, Symposium 1-S2-8, pp. 1-S2(21), Fukuoka, Mar. 2008 (in Japanese).

[2] W. van Eck, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?," Computers & Security, Vol. 4, No. 4, pp. 269–286, 1985.

[3] NSA, "NACSIM 5000 TEMPEST Fundamentals," http://cryptome.org/nacsim-5000.htm.

[4] M. G. Kuhn and R. J. Anderson, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations," Information Hiding (Ed. D. Aucsmith) 1998, Lecture Notes in Computer Science 1525, pp. 124–142, 1998.

Yasunao Suzuki
Senior Research Engineer, EMC Technology Group, Energy Systems Project, NTT Energy and Environment Systems Laboratories.

He received the M.E. degree in physics from Tohoku University, Miyagi, in 1990. He joined NTT Transmission Systems Laboratories in 1990. Since then, he has mainly been engaged in research on WDM-based optical access network technologies. Since July 2006, he has been engaged in research on EMC and electromagnetic security in his present post. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan.

Masao Masugi
Senior Research Engineer, NTT Energy and Environment Systems Laboratories.

He received the B.E., M.E., and Dr.Eng. degrees in electrical engineering from Keio University, Kanagawa, in 1987, 1989, and 1994, respectively. He joined NTT Electrical Telecommunication Laboratory in 1989. His research field has been in the measurement and analysis of time series signals in EMC fields, QoS evaluation of network and video streaming systems, and nonlinear analysis of Internet traffic. He received the Paper Presentation Award from the Institute of Electrical Engineers of Japan in 1992.

Kimihiro Tajima
Senior Manager, Research and Development Planning Department, NTT.

He received the B.E. and M.E. degrees from the Department of Electronics at Kumamoto University, Kumamoto, in 1986 and 1989, respectively. He joined NTT Telecommunications Networks Laboratories in 1989. He has been engaged in studies on optical-scheme-based measuring methods in the EMC field, development of mobile communication systems using infrared rays for EMC, etc. He is a secretary of the Japanese National Committee of CISPR Group A and of the Technical Committee on Electromagnetic Compatibility of IEICE. He is a member of IEEE. He moved from the ECM Technology Group, Energy Systems Project, NTT Energy and Environment Systems Laboratories, to his current department in July 2008.

Hiroshi Yamane
Senior Research Engineer, NTT Energy and Environment Systems Laboratories.

He received the B.E. and Dr.Eng. degrees in electrical engineering from Ibaraki University, Ibaraki, in 1980 and 1997, respectively. He joined NTT Electrical Telecommunication Laboratory, Nippon Telegraph and Telephone Public Corporation (now NTT) in 1980. His research fields have included the design of lightning surge protection methods for telecommunication network systems and the development of earthing and shielding systems against overvoltage problems in the EMC field. He received the Shibusawa Award from the Japan Electric Association in 2003.